UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/825,827	04/16/2004	Jeremy Stieglitz	50325-0874	9440

29989 7590 04/13/2010

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	PAPER NUMBER
2431	
MAIL DATE	DELIVERY MODE
04/13/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/825,827	STIEGLITZ ET AL.	
	Examiner	Art Unit	
	KAVEH ABRISHAMKAR	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 February 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14,16-33,35-49,51-67 and 69-71* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14, 16-33, 35-49, 51-67, and 69-71* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on February 24, 2010 has been entered.

1. Claims 1-14, 16-33, 35-49, 51-67, and 69-71 are currently pending consideration.

Response to Arguments

Applicant's arguments filed on June 30, 2009 have been fully considered but they are not persuasive for the following reasons:

Regarding claim 1, the Applicant argues that the Cited Prior Art (CPA), Kumhyr in view of Wood does not disclose "if the password does not meet the quality criteria granting a different level of access than if the password meets the quality criteria." The Examiner used a 103 rejection, and introduced Wood to teach this limitation. Wood teaches different levels of trust (different level of access) based on the authentication credentials (column 17, lines 45-60). These credentials can be username/password pairs (column 17, lines 45-47). Since the password is part of the credentials which are used to grant varying levels of trust, it is respectfully asserted that the password is tied

to the trust level and therefore to the different level of access. Therefore, the argument is not found persuasive. Furthermore, the Applicant argues that the CPA, White, does not teach determining whether the password meets quality criteria comprising determining whether the password meets quality criteria for a particular user role. White was used only for associating passwords with user roles (White: column 9, lines 5-18). However, Wood was still staid to disclose different trust levels with users (Wood: column 17, lines 45-60). Therefore, it would have been obvious to relate the password with the user role according to White, but the password being associated with the level of access is taught by Wood (Wood: column 17, lines 45-60). Therefore, the arguments are not found persuasive, and the rejection is maintained as given below.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-12, 16-31, 35-47, 51-66, and 69-71 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kumhyr (U.S. Patent Pub. No. US 2004/0250139 A1) in view of Wood et al. (U.S. Patent 6,944,761) in further in view of White (U.S. Patent 6,826,692).

Regarding claim 1, Kumhyr discloses:

A method of dynamically mitigating a noncompliant password, the method comprising the machine-implemented steps of:

obtaining a password from a user when the user attempts to access a service (paragraph 0026: *receives a password*);

determining whether the password meets quality criteria (paragraph 0026: *checks the password for compliance with format specification*);

if the password does not meet the quality criteria, performing one or more responsive actions that relate to accessing the service (paragraph 0027: *wherein if the password does not comply, a responsive action is taken*)

wherein the method is performed by one or more computing devices.

Kumhyr does not explicitly disclose granting a first level of access based on a first quality criteria, and granting a second level of access based on meeting a second level of quality criteria. Wood teaches granting different levels of trust level based on the authentication information (passwords) (Wood: column 17, lines 45-60). It would have been obvious to use the method of providing different levels of access with different passwords to provide an "authentication level commensurate with the authentication requirements of at least one of the information resources" (Wood: column 4, lines 7-13).

Wood and Kumhyr do not explicitly disclose that the user is associated with a particular user role, and wherein determining the password meets quality criteria is determining whether the password meets quality criteria for the user role. White, in an

analogous art, discloses that a password is associated with a user role which will determine to what services that user is allowed access (White: column 9, lines 5-18). Wood discloses different trust levels associated with users, but does not directly assign a role each user based on the password. It would have been obvious to add this functionality to the system of Wood-Kumhyr to allow a user logged onto the network to access an assortment of network services based on the user's role (White: column 5, lines 13-18).

Claim 2 is rejected as applied above in rejecting claim 1. Kumhyr does not explicitly disclose granting a first level of access based on a first quality criteria, and granting a second level of access based on meeting a second level of quality criteria. Wood teaches granting different levels of trust level based on the authentication information (passwords) (Wood: column 17, lines 45-60). It would have been obvious to use the method of providing different levels of access with different passwords to provide an "authentication level commensurate with the authentication requirements of at least one of the information resources" (Wood: column 4, lines 7-13).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Kumhyr discloses:

The method of claim 1, wherein the step of performing one or more responsive actions that relate to accessing the service comprises performing one or more of:

logging information related to the password;

sending a report about the password;

generating an alert about the password; forcing a password change; or

blocking the user's access to the service (paragraph 0027: *wherein the password is adjusted to meet the specifications*).

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Kumhyr discloses:

The method of claim 1, wherein the method further comprises, if the password does meet the quality criteria, providing user access to the service (paragraph 0026: *wherein if the password meets the specifications, the password is forwarded to the specified application*).

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Kumhyr discloses:

The method of claim 1, wherein the step of determining whether the password meets quality criteria further comprises one or more of the steps of:

performing a dictionary look-up based on the one or more symbols used in the password;

checking the length of the one or more symbols used in the password;

checking the number of unique characters of the one or more symbols used in the password;

checking the case of the characters in the one or more symbols used in the password;

checking the sequencing of characters in the one or more symbols used in the password; or

performing statistical analysis based on the one or more symbols used in the password (paragraph 0027: *wherein the number of characters may be adjusted*).

Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, Kumhyr discloses:

The method of claim 1, wherein the step of performing one or more responsive actions that relate to accessing the service comprises logging information related to the password (paragraph 0027).

Claim 7 is rejected as applied above in rejecting claim 1. Furthermore, Kumhyr discloses:

The method of claim 1, wherein the step of performing one or more responsive actions that relate to accessing the service comprises sending a report about the password (paragraph 0027: wherein the password is determined to match up with a password format specification).

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Kumhyr discloses:

The method of claim 1, wherein the step of performing one or more responsive actions that relate to accessing the service comprises generating an alert about the password (paragraph 0027: *wherein the password is determined to match up with a password format specification*).

Claim 9 is rejected as applied above in rejecting claim 1. Furthermore, Kumhyr discloses:

The method of claim 1, wherein the step of performing one or more responsive actions that relate to accessing the service comprises forcing a password change (paragraph 0027: *wherein the password is adjusted to meet the specifications*).

Claim 10 is rejected as applied above in rejecting claim 1. Furthermore, Kumhyr discloses:

The method of claim 1, wherein the step of performing one or more responsive actions that relate to accessing the service comprises blocking the user's access to the service (paragraph 0027: *wherein access to the application is not permitted if the password does not meet the format specifications*).

Claim 11 is rejected as applied above in rejecting claim 1. Furthermore, Kumhyr discloses:

The method of claim 1, wherein obtaining the password from the user comprises obtaining the password from the user via a graphical user interface (paragraph 0020: *receiving a password from a user*).

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Kumhyr discloses:

The method of claim 1, wherein obtaining the password from the user comprises obtaining the password from the user via an electronic interface (paragraph 0020: *receiving a password from a user*).

Claim 16 is rejected as applied above in rejecting claim 1. Furthermore, Kumhyr discloses:

The method of claim 1, wherein determining whether the password meets quality criteria comprises determining whether the password meets quality criteria for the service (paragraph 0026: *wherein the password is checked for compliance with a format specification* for a target application).

Claim 17 is rejected as applied above in rejecting claim 1. Furthermore, Kumhyr discloses:

The method of claim 1, wherein the step of obtaining the password comprises an access service obtaining the password from the user when the user attempts to access the service, and wherein the access service comprises machine executable instructions

executing on a particular machine, and the service comprises machine executable instruction executing on the same particular machine (paragraph 0026: wherein the password is to access a target application which could be on the same machine or a distinct machine).

Claim 18 is rejected as applied above in rejecting claim 1. Furthermore, Kumhyr discloses:

The method of claim 1, wherein the step of obtaining the password comprises an access service obtaining the password from the user when the user attempts to access the service, and wherein the access service comprises machine executable instructions executing on a first machine and the service comprises machine executable instructions executing on a second machine, wherein the first machine is distinct from the second machine (paragraph 0026: wherein the password is to access a target application which could be on the same machine or a distinct machine).

Regarding claim 19, Kumhyr discloses:

A method of dynamically mitigating a noncompliant password, the method comprising the machine-implemented steps of:

obtaining a password from a user when the user attempts to access a service (paragraph 0026: *receives a password*);

determining whether the password meets quality criteria (paragraph 0026: *checks the password for compliance with format specification*); and

if the password does not meet the quality criteria, performing one or more of:

forcing a password change (paragraph 0027: *wherein the password is adjusted to meet the specifications*); or

blocking the user's access to the service; and

wherein the step of determining whether the password meets quality criteria further comprises one or more of the steps of:

performing a dictionary look-up based on the one or more symbols used in the password;

checking the length of the one or more symbols used in the password;

checking the number of unique characters of the one or more symbols used in the password;

checking the case of the characters in the one or more symbols used in the password;

checking the sequencing of characters in the one or more symbols used in the password; or

performing statistical analysis based on the one or more symbols used in the password (paragraph 0027: *wherein the number of characters may be adjusted*).

Kumhyr does not explicitly disclose granting a first level of access based on a first quality criteria, and granting a second level of access based on meeting a second level of quality criteria. Wood teaches granting different levels of trust level based on the authentication information (passwords) (Wood: column 17, lines 45-60). It would have been obvious to use the method of providing different levels of access with

different passwords to provide an "authentication level commensurate with the authentication requirements of at least one of the information resources" (Wood: column 4, lines 7-13).

Wood and Kumhyr do not explicitly disclose that the user is associated with a particular user role, and wherein determining the password meets quality criteria is determining whether the password meets quality criteria for the user role. White, in an analogous art, discloses that a password is associated with a user role which will determine to what services that user is allowed access (White: column 9, lines 5-18). Wood discloses different trust levels associated with users, but does not directly assign a role each user based on the password. It would have been obvious to add this functionality to the system of Wood-Kumhyr to allow a user logged onto the network to access an assortment of network services based on the user's role (White: column 5, lines 13-18).

Regarding claim 20, Kumhyr discloses:

A machine-readable medium carrying one or more sequences of instructions for dynamically mitigating a noncompliant password, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

obtaining a password from a user when the user attempts to access a service (paragraph 0026: *receives a password*);

determining whether the password meets quality criteria (paragraph 0026: *checks the password for compliance with format specification)*; and

if the password does not meet the quality criteria, performing one or more responsive actions that relate to accessing the service (paragraph 0027: *wherein if the password does not comply, a responsive action is taken*).

Kumhyr does not explicitly disclose granting a first level of access based on a first quality criteria, and granting a second level of access based on meeting a second level of quality criteria. Wood teaches granting different levels of trust level based on the authentication information (passwords) (Wood: column 17, lines 45-60). It would have been obvious to use the method of providing different levels of access with different passwords to provide an "authentication level commensurate with the authentication requirements of at least one of the information resources" (Wood: column 4, lines 7-13).

Wood and Kumhyr do not explicitly disclose that the user is associated with a particular user role, and wherein determining the password meets quality criteria is determining whether the password meets quality criteria for the user role. White, in an analogous art, discloses that a password is associated with a user role which will determine to what services that user is allowed access (White: column 9, lines 5-18). Wood discloses different trust levels associated with users, but does not directly assign a role each user based on the password. It would have been obvious to add this functionality to the system of Wood-Kumhyr to allow a user logged onto the network to access an assortment of network services based on the user's role (White: column 5, lines 13-18).

Claim 21 is rejected as applied above in rejecting claim 20. Kumhyr does not explicitly disclose granting a first level of access based on a first quality criteria, and granting a second level of access based on meeting a second level of quality criteria. Wood teaches granting different levels of trust level based on the authentication information (passwords) (Wood: column 17, lines 45-60). It would have been obvious to use the method of providing different levels of access with different passwords to provide an "authentication level commensurate with the authentication requirements of at least one of the information resources" (Wood: column 4, lines 7-13).

Claim 22 is rejected as applied above in rejecting claim 20. Furthermore, Kumhyr discloses:

The machine-readable medium of claim 20, wherein the step of performing one or more responsive actions that relate to accessing the service comprises performing one or more of:

logging information related to the password;

sending a report about the password;

generating an alert about the password;

forcing a password change; or

blocking the user's access to the service (paragraph 0027: *wherein the password is adjusted to meet the specifications*).

Claim 23 is rejected as applied above in rejecting claim 20. Furthermore, Kumhyr discloses:

The machine-readable medium of claim 20, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to carry out the step of, if the password does meet the quality criteria, providing user access to the service (paragraph 0026: *wherein if the password meets the specifications, the password is forwarded to the specified application*).

Claim 24 is rejected as applied above in rejecting claim 20. Furthermore, Kumhyr discloses:

The machine-readable medium of claim 20, wherein the step of determining whether the password meets quality criteria further comprises one or more of the steps of: performing

a dictionary look-up based on the one or more symbols used in the password;

checking the length of the one or more symbols used in the password;

checking the number of unique characters of the one or more symbols used in the password;

checking the case of the characters in the one or more symbols used in the password;

checking the sequencing of characters in the one or more symbols used in the password; or

performing statistical analysis based on the one or more symbols used in the password (paragraph 0027: *wherein the number of characters may be adjusted*).

Claim 25 is rejected as applied above in rejecting claim 20. Furthermore, Kumhyr discloses:

The machine-readable medium of claim 20, wherein the step of performing one or more responsive actions that relate to accessing the service comprises logging information related to the password (paragraph 0027).

Claim 26 is rejected as applied above in rejecting claim 20. Furthermore, Kumhyr discloses:

The machine-readable medium of claim 20, wherein the step of performing one or more responsive actions that relate to accessing the service comprises sending a report about the password (paragraph 0027: wherein the password is determined to match up with a password format specification).

Claim 27 is rejected as applied above in rejecting claim 20. Furthermore, Kumhyr discloses:

The machine-readable medium of claim 20, wherein the step of performing one or more responsive actions that relate to accessing the service comprises generating an alert about the password (paragraph 0027: *wherein the password is determined to match up with a password format specification*).

Claim 28 is rejected as applied above in rejecting claim 20. Furthermore, Kumhyr discloses:

The machine-readable medium of claim 20, wherein the step of performing one or more responsive actions that relate to accessing the service comprises forcing a password change (paragraph 0027: *wherein the password is adjusted to meet the specifications*).

Claim 29 is rejected as applied above in rejecting claim 20. Furthermore, Kumhyr discloses:

The machine-readable medium of claim 20, wherein the step of performing one or more responsive actions that relate to accessing the service comprises blocking the user's access to the service (paragraph 0027: *wherein access to the application is not permitted if the password does not meet the format specifications*).

Claim 30 is rejected as applied above in rejecting claim 20. Furthermore, Kumhyr discloses:

The machine-readable medium of claim 20, wherein obtaining the password from the user comprises obtaining the password from the user via a graphical user interface (paragraph 0020: *receiving a password from a user*).

Claim 31 is rejected as applied above in rejecting claim 20. Furthermore, Kumhyr discloses:

The machine-readable medium of claim 20, wherein obtaining the password from the user comprises obtaining the password from the user via an electronic interface (paragraph 0020: *receiving a password from a user*).

Claim 35 is rejected as applied above in rejecting claim 20. Furthermore, Kumhyr discloses:

The machine-readable medium of claim 20, wherein determining whether the password meets quality criteria comprises determining whether the password meets quality criteria for the service (paragraph 0026: *wherein the password is checked for compliance with a format specification* for a target application).

Regarding claim 36, Kumhyr discloses:

An apparatus for dynamically mitigating a noncompliant password, comprising:

means for obtaining a password from a user when the user attempts to access a service (paragraph 0026: *receives a password*);

means for determining whether the password meets quality criteria (paragraph 0026: *checks the password for compliance with format specification)*; and

means for performing one or more responsive actions that relate to accessing the service if the password does not meet the quality criteria (paragraph 0027: *wherein if the password does not comply, a responsive action is taken*).

Wood and Kumhyr do not explicitly disclose that the user is associated with a particular user role, and wherein determining the password meets quality criteria is determining whether the password meets quality criteria for the user role. White, in an analogous art, discloses that a password is associated with a user role which will determine to what services that user is allowed access (White: column 9, lines 5-18). Wood discloses different trust levels associated with users, but does not directly assign a role each user based on the password. It would have been obvious to add this functionality to the system of Wood-Kumhyr to allow a user logged onto the network to access an assortment of network services based on the user's role (White: column 5, lines 13-18).

Claim 37 is rejected as applied above in rejecting claim 36. Kumhyr does not explicitly disclose granting a first level of access based on a first quality criteria, and granting a second level of access based on meeting a second level of quality criteria. Wood teaches granting different levels of trust level based on the authentication information (passwords) (Wood: column 17, lines 45-60). It would have been obvious to use the method of providing different levels of access with different passwords to provide an "authentication level commensurate with the authentication requirements of at least one of the information resources" (Wood: column 4, lines 7-13).

Claim 38 is rejected as applied above in rejecting claim 36. Furthermore, Kumhyr discloses:

The apparatus of claim 36, wherein the means for performing one or more responsive actions that relate to accessing the service comprises one or more of:

means for logging information related to the password;

means for sending a report about the password;

means for generating an alert about the password;

means for forcing a password change; or

means for blocking the user's access to the service (paragraph 0027: *wherein the password is adjusted to meet the specifications*).

Claim 39 is rejected as applied above in rejecting claim 36. Furthermore, Kumhyr discloses:

The apparatus of claim 36, wherein the apparatus further comprises means for providing user access to the service if the password does meet the quality criteria (paragraph 0026: *wherein if the password meets the specifications, the password is forwarded to the specified application*).

Claim 40 is rejected as applied above in rejecting claim 36. Furthermore, Kumhyr discloses:

The apparatus of claim 36, wherein the means for determining whether the password meets quality criteria further comprises one or more of:

means for performing a dictionary look-up based on the one or more symbols used in the password;

means for checking the length of the one or more symbols used in the password;

means for checking the number of unique characters of the one or more symbols used in the password;

means for checking the case of the characters in the one or more symbols used in the password;

means for checking the sequencing of characters in the one or more symbols used in the password; or

means for performing statistical analysis based on the one or more symbols used in the password (paragraph 0027: *wherein the number of characters may be adjusted*).

Claim 41 is rejected as applied above in rejecting claim 36. Furthermore, Kumhyr discloses:

The apparatus of claim 36, wherein the means for performing one or more responsive actions that relate to accessing the service comprises means for logging information related to the password (paragraph 0027).

Claim 42 is rejected as applied above in rejecting claim 36. Furthermore, Kumhyr discloses:

The apparatus of claim 36, wherein the means for performing one or more responsive actions that relate to accessing the service comprises means for sending a report about the password (paragraph 0027: *wherein the password is determined to match up with a password format specification*).

Claim 43 is rejected as applied above in rejecting claim 36. Furthermore, Kumhyr discloses:

The apparatus of claim 36, wherein the means for performing one or more responsive actions that relate to accessing the service comprises means for generating an alert about the password (paragraph 0027: *wherein the password is determined to match up with a password format specification*).

Claim 44 is rejected as applied above in rejecting claim 36. Furthermore, Kumhyr discloses:

The apparatus of claim 36, wherein the means for performing one or more responsive actions that relate to accessing the service comprises means for forcing a password change (paragraph 0027: *wherein the password is adjusted to meet the specifications*).

Claim 45 is rejected as applied above in rejecting claim 36. Furthermore, Kumhyr discloses:

The apparatus of claim 36, wherein the means for performing one or more responsive actions that relate to accessing the service comprises means for blocking the user's access to the service (paragraph 0027: *wherein access to the application is not permitted if the password does not meet the format specifications*).

Claim 46 is rejected as applied above in rejecting claim 36. Furthermore, Kumhyr discloses:

The apparatus of claim 36, wherein the means for obtaining the password from the user comprises means for obtaining the password from the user via a graphical user interface (paragraph 0020: *receiving a password from a user*).

Claim 47 is rejected as applied above in rejecting claim 36. Furthermore, Kumhyr discloses:

The apparatus of claim 36, wherein the means for obtaining the password from the user comprises means for obtaining the password from the user via an electronic interface (paragraph 0020: *receiving a password from a user*).

Claim 51 is rejected as applied above in rejecting claim 36. Furthermore, Kumhyr discloses:

The apparatus of claim 36, wherein means for determining whether the password meets quality criteria comprises means for determining whether the password meets quality criteria for the service (paragraph 0026: *wherein if the password meets the specifications, the password is forwarded to the specified application*).

Claim 52 is rejected as applied above in rejecting claim 36. Furthermore, Kumhyr discloses:

The apparatus of claim 36, wherein the means for obtaining the password comprises means for an access service to obtain the password from the user when the user attempts to access the service, and wherein the access service comprises means for executing on a particular machine, and wherein the service comprises means for executing on the same particular machine (paragraph 0026: *wherein the password is to access a target application which could be on the same machine or a distinct machine*).

Claim 53 is rejected as applied above in rejecting claim 36. Furthermore, Kumhyr discloses:

The apparatus of claim 36, wherein the means for obtaining the password comprises means for an access service to obtain the password from the user when the user attempts to access the service, and wherein the access service comprises means for executing on a first machine and the service comprises means for executing on a second machine, wherein the first machine is distinct from the second machine (paragraph 0026: wherein the password is to access a target application which could be on the same machine or a distinct machine).

Regarding claim 54, Kumhyr discloses:

An apparatus for dynamically mitigating a noncompliant password, comprising:

a network interface that is coupled to the data network for receiving one or more packet flows therefrom (paragraph 0026);

a processor (paragraph 0026);

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

obtaining a password from a user when the user attempts to access a service (paragraph 0026: *receives a password*);

determining whether the password meets quality criteria (paragraph 0026: *checks the password for compliance with format specification*); and

if the password does not meet the quality criteria, performing one or more responsive actions that relate to accessing the service (paragraph 0027: *wherein if the password does not comply, a responsive action is taken*).

Kumhyr does not explicitly disclose granting a first level of access based on a first quality criteria, and granting a second level of access based on meeting a second level of quality criteria. Wood teaches granting different levels of trust level based on the authentication information (passwords) (Wood: column 17, lines 45-60). It would have been obvious to use the method of providing different levels of access with different passwords to provide an "authentication level commensurate with the authentication requirements of at least one of the information resources" (Wood: column 4, lines 7-13).

Wood and Kumhyr do not explicitly disclose that the user is associated with a particular user role, and wherein determining the password meets quality criteria is determining whether the password meets quality criteria for the user role. White, in an analogous art, discloses that a password is associated with a user role which will determine to what services that user is allowed access (White: column 9, lines 5-18).

Wood discloses different trust levels associated with users, but does not directly assign a role each user based on the password. It would have been obvious to add this functionality to the system of Wood-Kumhyr to allow a user logged onto the network to access an assortment of network services based on the user's role (White: column 5, lines 13-18).

Claim 55 is rejected as applied above in rejecting claim 54. Kumhyr does not explicitly disclose granting a first level of access based on a first quality criteria, and granting a second level of access based on meeting a second level of quality criteria. Wood teaches granting different levels of trust level based on the authentication information (passwords) (Wood: column 17, lines 45-60). It would have been obvious to use the method of providing different levels of access with different passwords to provide an "authentication level commensurate with the authentication requirements of at least one of the information resources" (Wood: column 4, lines 7-13).

Claim 56 is rejected as applied above in rejecting claim 54. Furthermore, Kumhyr discloses:

The apparatus of claim 54, wherein the step of performing one or more responsive actions that relate to accessing the service comprises performing one or more of:

logging information related to the password;

sending a report about the password;

generating an alert about the password;

forcing a password change; or

blocking the user's access to the service (paragraph 0027: *wherein the password is adjusted to meet the specifications*).

Claim 57 is rejected as applied above in rejecting claim 54. Furthermore, Kumhyr discloses:

The apparatus of claim 54, wherein the apparatus further comprises one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the step of, if the password does meet the quality criteria, providing user access to the service (paragraph 0026: *wherein if the password meets the specifications, the password is forwarded to the specified application*).

Claim 58 is rejected as applied above in rejecting claim 54. Furthermore, Kumhyr discloses:

The apparatus of claim 54, wherein the step of determining whether the password meets quality criteria comprises one or more of the steps of:

performing a dictionary look-up based on the one or more symbols used in the password;

checking the length of the one or more symbols used in the password;

checking the number of unique characters of the one or more symbols used in the password;

checking the case of the characters in the one or more symbols used in the password;

checking the sequencing of characters in the one or more symbols used in the password; or

performing statistical analysis based on the one or more symbols used in the password (paragraph 0027: *wherein the number of characters may be adjusted*).

Claim 59 is rejected as applied above in rejecting claim 54. Furthermore, Kumhyr discloses:

The apparatus of claim 54, wherein the step of performing one or more responsive actions that relate to accessing the service comprises logging information related to the password (paragraph 0027).

Claim 60 is rejected as applied above in rejecting claim 54. Furthermore, Kumhyr discloses:

The apparatus of claim 54, wherein the step of performing one or more responsive actions that relate to accessing the service comprises sending a report about the password (paragraph 0027: *wherein the password is determined to match up with a password format specification*).

Claim 61 is rejected as applied above in rejecting claim 54. Furthermore, Kumhyr discloses:

The apparatus of claim 54, wherein the step of performing one or more responsive actions that relate to accessing the service comprises generating an alert about the password (paragraph 0027: *wherein the password is determined to match up with a password format specification*).

Claim 62 is rejected as applied above in rejecting claim 54. Furthermore, Kumhyr discloses:

The apparatus of claim 54, wherein the step of performing one or more responsive actions that relate to accessing the service comprises forcing a password change (paragraph 0027: *wherein the password is adjusted to meet the specifications*).

Claim 63 is rejected as applied above in rejecting claim 54. Furthermore, Kumhyr discloses:

The apparatus of claim 54, wherein the step of performing one or more responsive actions that relate to accessing the service comprises blocking the user's access to the service (paragraph 0027: *wherein access to the application is not permitted if the password does not meet the format specifications*).

Claim 64 is rejected as applied above in rejecting claim 54. Furthermore, Kumhyr discloses:

The apparatus of claim 54, wherein obtaining the password from the user comprises obtaining the password from the user via a graphical user interface (paragraph 0020: *receiving a password from a user*).

Claim 65 is rejected as applied above in rejecting claim 54. Furthermore, Kumhyr discloses:

The apparatus of claim 54, wherein obtaining the password from the user comprises obtaining the password from the user via an electronic interface (paragraph 0020: *receiving a password from a user*).

Claim 69 is rejected as applied above in rejecting claim 54. Furthermore, Kumhyr discloses:

The apparatus of claim 54, wherein determining whether the password meets quality criteria comprises determining whether the password meets quality criteria for the service (paragraph 0026: *wherein if the password meets the specifications, the password is forwarded to the specified application*).

Claim 70 is rejected as applied above in rejecting claim 54. Furthermore, Kumhyr discloses:

The apparatus of claim 54, wherein the step of obtaining the password comprises an access service obtaining the password from the user when the user attempts to access the service, and wherein the access service comprises machine executable

instructions executing on the apparatus, and the service comprises machine executable instruction executing on the same apparatus (paragraph 0026: wherein the password is to access a target application which could be on the same machine or a distinct machine).

Claim 71 is rejected as applied above in rejecting claim 54. Furthermore, Kumhyr discloses:

The apparatus of claim 54, wherein the step of obtaining the password comprises an access service obtaining the password from the user when the user attempts to access the service, and wherein the access service comprises machine executable instructions executing on a first machine and the service comprises machine executable instructions executing on a second machine, wherein the first machine is distinct from the second machine (paragraph 0026: wherein the password is to access a target application which could be on the same machine or a distinct machine).

Claims 13, 32, 48, and 66 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kumhyr (U.S. Patent Pub. No. US 2004/0250139 A1) in view of Wood et al. (U.S. Patent 6,944,761) in further in view of White (U.S. Patent 6,826,692) in further in view of Hurley (U.S. Patent Pub. US 2004/0250139 A1).

Claim 13 is rejected as applied above in rejecting claim 1. Kumhyr-Wood-White does not explicitly disclose that a quality score is generated for a password, which is

compared to a threshold value. Hurley discloses a system using a quality meter which compares the quality of password to the minimum threshold, and if it does not meet it, a message is displayed (Hurley: paragraph 0030). Hurley and Kumhyr-Wood-White are analogous arts because both have to do with passwords and measuring their quality. It would have been obvious to one of ordinary skill in the art to use the quality meter of Hurley in the system of Kumhyr-Wood-White to check if a password is vulnerable to cracking and to notify the user on how to improve the quality (Hurley: paragraphs 0004-0005).

Claim 32 is rejected as applied above in rejecting claim 20. Kumhyr-Wood-White does not explicitly disclose that a quality score is generated for a password, which is compared to a threshold value. Hurley discloses a system using a quality meter which compares the quality of password to the minimum threshold, and if it does not meet it, a message is displayed (Hurley: paragraph 0030). Hurley and Kumhyr-Wood-White are analogous arts because both have to do with passwords and measuring their quality. It would have been obvious to one of ordinary skill in the art to use the quality meter of Hurley in the system of Kumhyr-Wood-White to check if a password is vulnerable to cracking and to notify the user on how to improve the quality (Hurley: paragraphs 0004-0005).

Claim 48 is rejected as applied above in rejecting claim 36. Kumhyr-Wood-White does not explicitly disclose that a quality score is generated for a password, which is

compared to a threshold value. Hurley discloses a system using a quality meter which compares the quality of password to the minimum threshold, and if it does not meet it, a message is displayed (Hurley: paragraph 0030). Hurley and Kumhyr-Wood-White are analogous arts because both have to do with passwords and measuring their quality. It would have been obvious to one of ordinary skill in the art to use the quality meter of Hurley in the system of Kumhyr-Wood-White to check if a password is vulnerable to cracking and to notify the user on how to improve the quality (Hurley: paragraphs 0004-0005).

Claim 66 is rejected as applied above in rejecting claim 54. Kumhyr-Wood-White does not explicitly disclose that a quality score is generated for a password, which is compared to a threshold value. Hurley discloses a system using a quality meter which compares the quality of password to the minimum threshold, and if it does not meet it, a message is displayed (Hurley: paragraph 0030). Hurley and Kumhyr-Wood-White are analogous arts because both have to do with passwords and measuring their quality. It would have been obvious to one of ordinary skill in the art to use the quality meter of Hurley in the system of Kumhyr to check if a password is vulnerable to cracking and to notify the user on how to improve the quality (Hurley: paragraphs 0004-0005).

Claims 14, 33, and 67 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kumhyr (U.S. Patent Pub. No. US 2004/0250139 A1) in view of

Wood et al. (U.S. Patent 6,944,761) in further in view of White (U.S. Patent 6,826,692) in further in view of Casco-Arias et al. (U.S. Patent Pub. No. US 2004/0250141 A1).

Claim 14 is rejected as applied above in rejecting claim 1. Furthermore, Kumhyr discloses:

making a first determination whether the password meets quality criteria (paragraph 0026: *wherein if the password meets the specifications, the password is forwarded to the specified application*);

storing in a particular machine-readable medium an indication of the first determination of the password (paragraph 0026: *wherein if the password meets the specifications, the password is forwarded to the specified application (machine))*)

wherein the step of determining whether the password meets quality criteria comprises accessing the particular machine-readable medium ((paragraph 0026: *wherein if the password meets the specifications, the password is forwarded to the specified application*).

Kumhyr does not explicitly disclose obtaining a password from a repository of passwords. Casco-Arias teaches a password repository to store passwords (Casco-Arias: paragraph 0019). The password repository of Casco-Arias could be used with the system of Kumhyr to store passwords which are generated. It would have been obvious to use the password repository of Casco-Arias in the system of Kumhyr so that "passwords may be centrally managed according to shared password policies" which

can provide "more uniform levels of password strength among the data processing systems and may allow a user to request and/or change passwords in a more consistent manner" (Casco-Arias: paragraph 0007).

Claim 33 is rejected as applied above in rejecting claim 20. Furthermore, Kumhyr discloses:

The machine-readable medium of claim 20, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of:

making a first determination whether the password meets quality criteria (paragraph 0026: *wherein if the password meets the specifications, the password is forwarded to the specified application*);

storing in a particular machine-readable medium an indication of the first determination of the password (paragraph 0026: *wherein if the password meets the specifications, the password is forwarded to the specified application (machine)*))

wherein the step of determining whether the password meets quality criteria comprises accessing the particular machine-readable medium ((paragraph 0026: *wherein if the password meets the specifications, the password is forwarded to the specified application*).

Kumhyr does not explicitly disclose obtaining a password from a repository of passwords. Casco-Arias teaches a password repository to store passwords (Casco-

Arias: paragraph 0019). The password repository of Casco-Arias could be used with the system of Kumhyr to store passwords which are generated. It would have been obvious to use the password repository of Casco-Arias in the system of Kumhyr so that "passwords may be centrally managed according to shared password policies" which can provide "more uniform levels of password strength among the data processing systems and may allow a user to request and/or change passwords in a more consistent manner" (Casco-Arias: paragraph 0007).

Claim 67 is rejected as applied above in rejecting claim 54. Furthermore, Kumhyr discloses:

The apparatus of claim 54, further comprising one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

making a first determination whether the password meets quality criteria (paragraph 0026: *wherein if the password meets the specifications, the password is forwarded to the specified application*);

storing in a particular machine-readable medium an indication of the first determination of the password (paragraph 0026: *wherein if the password meets the specifications, the password is forwarded to the specified application (machine))*)

wherein the step of determining whether the password meets quality criteria comprises accessing the particular machine-readable medium ((paragraph 0026:

wherein if the password meets the specifications, the password is forwarded to the specified application).

Kumhyr does not explicitly disclose obtaining a password from a repository of passwords. Casco-Arias teaches a password repository to store passwords (Casco-Arias: paragraph 0019). The password repository of Casco-Arias could be used with the system of Kumhyr to store passwords which are generated. It would have been obvious to use the password repository of Casco-Arias in the system of Kumhyr so that "passwords may be centrally managed according to shared password policies" which can provide "more uniform levels of password strength among the data processing systems and may allow a user to request and/or change passwords in a more consistent manner" (Casco-Arias: paragraph 0007).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAVEH ABRISHAMKAR whose telephone number is (571)272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kaveh Abrishamkar/
Primary Examiner, Art Unit 2431

/K. A./
04/11/2010
Primary Examiner, Art Unit 2431